Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report
for 04 April 2003

Daily Overview

- The Associated Press reports the theft of nine devices used to derail railroad cars has prompted federal authorities to issue a bulletin to area law enforcement agencies in Louisiana. (See item 6)

- The Government Accounting Office has released GAO−03−616T, "Transportation Security: Post−9/11 Initiatives and Long−Term Challenges." (See item 8)

- The Associated Press reports that when a false Internet story about Severe Acute Respiratory Syndrome sent panic through much of Hong Kong, authorities sent a blanket text message to about six million mobile phones that denied the territory had been declared an "infected city." (See item 20)

- CNET News.com reports there are serious security holes in the popular digital media players QuickTime and RealPlayer, but in both cases updates are available to remedy the problem. (See item 22)

- ISS has raised its AlertCon level to 2 as a result of ISS X−Force being able to construct and test a fully functional and robust remote exploit for Sendmail.

DHS/IAIP Update *Fast Jump*

Production Industries: **Energy**; **Chemical**; **Defense Industrial Base**

Service Industries: **Banking and Finance**; **Transportation**; **Postal and Shipping**

Sustenance and Health: **Agriculture**; **Food**; **Water**; **Public Health**

Federal and State: **Government**; **Emergency Services**

IT and Cyber: **Information and Telecommunications**; **Internet Alert Dashboard**

Other: **General**; **DHS/IAIP Web Information**

Energy Sector

1. *April 03, Platts Global Energy News* — **No end in sight for Niger Delta oil field stand−off. Nigeria's crude output, which is running at nearly 38% below normal levels as a result of ethnic clashes in the western Niger Delta, is unlikely to be fully back on stream until after this month's elections,** oil industry officials said Thursday. "This has become a very political issue but the president has his hands full at the moment and it would appear his cabinet has advised him to hold of on the Delta situation until after the elections," a Lagos−based oil company official said. Three oil multinationals, Shell, ChevronTexaco and TotalFinaElf, shut down part of their operations three weeks ago after an uprising by ethnic Ijaw militants in the swamps south and west of the oil city of Warri triggered violent clashes with security forces. The Nigerian army says that peace has returned to the strife−torn area and some officials believe the government is banking on its ability to convince the companies that area is safe and to return before elections. **But the oil majors Thursday said they were not ready to restart production despite assurances from the armed forces that the unrest has been brought under control.**
Source: http://www.platts.com/stories/oil4.html

2. *April 02, Richmond Times−Dispatch* — **Virginia residents voice concerns over nuclear plant expansion proposal. Bad roads, a drought−shrunken lake and radioactive waste were among concerns raised yesterday at a public meeting on the potential expansion of the North Anna Nuclear Power Station.** Lake Anna provides cooling water to the two nuclear reactors at Dominion Virginia Power's North Anna power plant. Dominion plans to apply in September for NRC approval of a site at the plant where additional nuclear reactors could be built. The utility has stressed, though, that it has no plans to build additional reactors. Andrew Kugler, an NRC official responsible for environmental issues, responded to one question by offering assurances that additional hot water dumped into the lake from the reactor−cooling process would be considered in the review. Low lake levels that accompanied last year's drought would be examined, too, he said. **Others questioned why the handling of nuclear waste from possible additional reactors would not be considered in the permitting process. They were told that the NRC has determined that waste would not be an issue because a national waste repository would be available by 2025. Some questioned the security of waste that has been accumulating at the plant since its reactors began operating in 1978 and 1980.** NRC official Mike Scott responded that the agency has re−evaluated its security guidelines since the Sept. 11, 2001, terrorist attacks and required interim security measures that it believes provide effective security. **No nuclear power projects have been started in the United States since the accident at the Three Mile Island plant in Pennsylvania in 1979.**
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3748436

3. *April 02, The Wisconsin State Journal* — **Wisconsin power plant 's unplanned shutdowns cause regulators concern. Two organizations are asking state regulators to open an investigation into the Columbia power plant near Portage, WI, saying a large number of unplanned shutdowns is costing customers millions of dollars.** Meanwhile, the state Public Service Commission already has its eye on the plant's performance and has asked for voluminous records. "There are some concerns with the plant," spokeswoman Annemarie Newman said. **The power plant is in the midst of its seventh forced outage so far this year, and each day Columbia is down, it's costing ratepayers of the three utilities that own it**

about $1 million to buy replacement power, the Citizens Utility Board (CUB) and the Wisconsin Industrial Energy Group said Tuesday. "What happens when we get into the warm weather?" CUB executive director Steve Hiniker asked. "This is not a good sign." Columbia is one of the workhorse power plants that Madison Gas and Electric Co. and Alliant Energy Corp. depend on for their daily electricity needs. **The coal–fired plant can generate about 1,000 megawatts of power, enough to light about 250,000 homes.**
Source: http://www.energycentral.com/sections/news/nw_article.cfm?id =3748629

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

4. *April 03, New York Times* — **Thin work force of North Dakota gets thinner as residents go to war.** All across the sparsely populated plains of North Dakota, the invasion of Iraq is taking a toll on a state where enlistment is high and where younger people had already been leaving in search of work elsewhere. **Part–time military service is considered a good deal in North Dakota's cyclical and depressed rural economy.** "If you start talking a hundred dollars a day for a family man, that's good money for him," said Dale Moser, who has been the top recruiter for North Dakota's National Guard for three years running. In addition, they receive educational benefits, health insurance and supplementary income. **The costs of that bargain come during war. North Dakota now has 1,550 members of the reserve and National Guard suddenly activated –– approximately one out of every 250 people between the ages of 18 and 65. That exodus is leaving gaping holes in the social structure. To help ease the strain, the state government is considering a campaign to encourage people to take on additional part–time jobs and to get retirees back to the workplace.**
Source: http://www.nytimes.com/2003/04/03/international/worldspecial /03DAKO.html

[Return to top]

Banking and Finance Sector

5. *April 03, Washington Post* — **War exemption limits terrorism insurance.** More U.S. businesses and commercial property owners have been buying terrorism insurance since the start of the war in Iraq, insurance companies say, but it is not clear whether any damage they suffer would be covered, because of the "act of war" exclusion in most insurance policies. **The law Congress passed last fall requiring companies to offer the coverage does not address attacks that occur during hostilities, such as Iraq, that were not declared a war by Congress. The Treasury secretary would determine whether an attack was a terrorist act, enabling insurance companies to get help from the federal government in paying claims. If an act is not deemed terrorism, insurance companies could invoke the war exemption, industry experts said.** "We have reason to believe we could get hit with more terrorist attacks

than before the war began," said Harold D. Skipper Jr., a professor of risk management and insurance at Georgia State University. "But just because we get hit with them doesn't mean they are coming from Iraq or from war. We still have a lot of potential to continue to employ attorneys." **The law requires that a terrorist act be committed by a foreign source and occur in the United States for insurance companies to get federal aid. It also sets a threshold for government involvement based on a formula that takes into account the value of premiums that an insurer collects.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A15814−2003Apr 2.html

[Return to top]

Transportation Sector

6. *April 03, Associated Press* — **Nine train derailment devices stolen. The theft of nine devices used to derail railroad cars has prompted federal authorities to issue a bulletin to area law enforcement agencies in Louisiana. The devices "seems to have a solitary usage – to derail trains," said Mike Moriarty, chief deputy U.S. marshal.** "Since there are so many of them missing and we have such a high amount of railroad traffic through this area, it bears our notice," Moriarty said. **Since January, seven of the derailing devices were taken from the Greenville, Texas, area, one from near Lake Hubbard just east of Dallas and one from a Kansas City Southern rail yard in Winnsboro, Texas.** There have been no reported thefts of derailing equipment in Louisiana, Moriarty said. The derailing devices, portable hinged−type blocks, are used to prevent equipment from accidentally rolling onto the main rail route from a secondary track. "The railroad industry is aware of this. They shared this information immediately. And we're trying to make sure law enforcement is aware of it as well," Moriarty said. "And since these devices are so identifiable, we feel the public should know." **Moriarty said the devices were a serious security threat. "The devices are quite small and can be deployed by one individual and could create havoc with any train," he said.**
Source: http://www.nola.com/newsflash/louisiana/index.ssf?/newsflash /get_story.ssf?/cgi−free/getstory_ssf.cgi?n1427_BC_LA−−Derai lmentDeviceslouisiana

7. *April 03, Reuters* — **Treasury tells airlines to cut costs.** U.S. Treasury Secretary John Snow said on Thursday that the troubled airline industry needs to cut its costs and not rely on government aid. "The administration has made clear...don't depend on us to solve these problems," Snow said after a luncheon address to the Orlando Chamber of Commerce. **Snow said all the participants in the U.S. airline industry must get their costs in line with their revenues and said this would require an industry−wide restructuring.** Airlines, which had already projected nearly $7 billion in losses for 2003, have recently warned that a fuel price spike and steep travel declines over three months could produce an additional $4 billion in losses. **Since the war began, they have slashed thousands of flights, cut 10,000 jobs and warned of more potential bankruptcies.**
Source: http://www.msnbc.com/news/895037.asp?cp1=1

8. *April 01, Government Accounting Office* — **GAO−03−616T: Transportation Security: Post−9/11 Initiatives and Long−Term Challenges.** On April 1, the Government Accounting Office released GAO−03−616T, Testimony by Gerald L. Dillingham, director, physical infrastructure, before the National Commission on Terrorist Attacks Upon the United States, in

New York, New York. **This testimony responds to the request of the National Commission on Terrorist Attacks Upon the United States for information on GAO's work in transportation security.** It addresses such matters as what the federal government has done since September 11, to strengthen transportation security, particularly aviation, mass transit, and port security. This testimony does not contain recommendations. **However, GAO reports and testimonies on aviation, transit, and port security and on management issues are listed at the end of the statement.** Many of these reports and testimonies contain GAO recommendations. Highlights: http://www.gao.gov/highlights/d03616thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−03−616T

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

9. *April 03, Associated Press* — **Cattle disease gains more attention. A voluntary testing program for Johne's disease should be expanded, says Dr. Sam Holland, state veterinarian.** Holland, who is executive secretary of the South Dakota Animal Industry Board, says the board has proposed paying for follow−up testing on cattle that are suspected of having the disease. **New rules also would allow the board to help finance herd−management plans, he says.** "There are some producers that know they have the disease in their herds, and rather than spend a lot of money on testing, they'd like to do more management to control and eliminate the disease," Holland says.
Source: http://www.aberdeennews.com/mld/aberdeennews/news/5548318.ht m

10. *April 03, icNewcastle* — **U.S. laboratory hoping to market live tests for BSE. The first test for bovine spongiform encephalitis (BSE) in live cattle could potentially be on the market within 18 months, under a licensing agreement announced Wednesday. At present, farmers who suspect one of their cows is suffering from BSE must have the animal slaughtered to enable it to be tested.** But a UK firm announced yesterday that it has signed an agreement licensing a U.S. veterinary giant to develop and produce tests which could make slaughter unnecessary. The company has developed a range of "biomarkers" which, it says, can detect BSE and equivalent diseases in other live animals, such as scrapie in sheep.
Source: http://icnewcastle.icnetwork.co.uk/0100news/0107farming/page .cfm?objectid=12803838id=50081

[Return to top]

Food Sector

11. *April 03, Food Production Daily* — **FDA readies for registration of all international food suppliers. Food producers across the globe are being urged to register as soon as possible**

with the U.S. Food and Drug Administration (FDA) in order to comply with the imminent Public Health Security and Bioterrorism Preparedness and Response Act of 2002. The legislation aims to provide the FDA with new authority to protect the U.S. food supply against terrorist acts and other public health threats. It allows the FDA wider inspection powers to ensure the safety of imported food products before they enter the U.S. **More than 400,000 commercial operations worldwide are estimated to be affected by the new rules.** Under the terms of the Act, owners, operators, or agents in−charge of a domestic or foreign facility must submit a registration to the FDA. In it they must record the trading name of the business, the name and address of each of its facilities, the business and food categories the facility handles and, for overseas operations, details of the U.S. agent.
Source: http://www.foodproductiondaily.com/news/news.asp?id=2582

[Return to top]

Water Sector

12. *April 02, Associated Press* — **Waste spill cuts water supply to more than a half million people in Brazil. A massive spill of caustic soda in two southeastern rivers prompted authorities to cut off water supplies to some 550,000 people Wednesday, the Brazilian government said.** The Rio de Janeiro government ordered eight artesian wells drilled and sent trucks to supply drinking water to seven cities and towns affected by the spill. The waste was moving toward the Atlantic Ocean at a rate of about 30 metres a minute, state officials said. On Wednesday it reached Campos, a city of 300,000 about 65 kilometres from the sea. **The accident occurred last weekend when a reservoir used to store chemical waste burst at an abandoned paper and pulp plant in Cataguazes, in neighbouring Minas Gerais state. The residue flowed into the Pomba and Paraiba do Sul rivers, which run through Rio de Janeiro.**
Source: http://www.canada.com/news/story.asp?id=%7B89708F6B−DFA8−45A 9−BC2B−1C6B3ED40942%7D

[Return to top]

Public Health Sector

13. *April 04, Hindu* — **India to screen air passengers for SARS virus.** The Indian government decided Thursday to screen passengers from all the countries at airports for the symptoms related to an unknown pneumonia rather than limiting it to those from where the virus has been reported, officials said today. This was being done in view of the Severe Acute Respiratory Syndrome (SARS) now being reported from more countries, 18 in all, Joint Secretary in the Health Ministry Bhavani Thyagrajan said. **"No case has been reported in the country," she said, adding the Government had also decided to get filled a proforma by all passengers disembarking in India rather than only by those from countries in which infection has spread.**
Source: http://www.hinduonnet.com/thehindu/holnus/01032218.htm

14.

April 03, CBS News — **Terror weapons in the cupboard.** Terrorists could use common household items to improvise chemical or biological weapons and then hide them in food. **Using materials available at stores, on the Internet or through mail−order firms, terrorists could make cyanide compounds, grow salmonella bacteria and botulinum toxin, or distill the poison ricin from castor beans.** Yeast, infant formula, sugar, Epsom Salts, cheesecloth, blenders, masks and gloves are among the items widely available that terrorists could use to set up a laboratory to make crude chemical and biological weapons. **Detection of these home−made labs is often difficult because so many household products can be used in production, and the recipes are readily available on the Internet.**
Source: http://www.cbsnews.com/stories/2003/04/03/attack/main547501. shtml

15. *April 03, Scripps Howard News Service* — **Test shows promise in detecting SARS. Although it's not a sure thing, federal authorities have begun offering the first lab test to help state and local health officials determine whether patients may have the dangerous new respiratory disease spreading around the globe.** Julie Gerberding, director of the U.S. Centers for Disease Control and Prevention, said Wednesday that the process "takes some time." It requires at least two samples from a patient to determine if the person has antibodies to a coronavirus that's the leading suspect as the cause of the flu−like illness. **"There's an association to Severe Acute Respiratory Syndrome (SARS) and this new coronavirus, but we're not yet calling this a confirmation of SARS until we get a lot more experience with the tests," Gerberding said.**
Source: http://www.insidevc.com/vcs/national/article/0,1375,VCS_123_1861075,00.html

[Return to top]

Government Sector

16. *April 03, Washington Post* — **More funds sought for homeland security.** Senate Democrats yesterday launched a drive to double President Bush's request for homeland security funds as part of a nearly $80 billion measure to finance the war in Iraq, combat terrorism and help the nation's financially troubled airlines. **The Senate voted 52 to 47, largely along party lines, to reject a proposal from Sen. Ernest F. Hollings (D−S.C.) to add $1 billion to strengthen port security, including grants for security operations, radiation detection equipment and more resources for the Coast Guard.** Key Republicans said they favor providing more funds for port security, but not in this bill. The Senate, with support from leaders of both parties, is pushing to pass the $78.7 billion measure by late Thursday. The House plans to take up and pass its $77.9 billion version of the legislation today. The bills, approved Tuesday by House and Senate appropriations committees, include Bush's request of roughly $4 billion for homeland security. **Senate Democrats are trying to reconfigure and raise that amount to $9 billion, largely to increase spending for police, firefighters and other first responders and for high−risk area such as New York and Washington.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A14842−2003Apr 2.html

17. *April 01, Department of Homeland Security* — **Establishment of the Homeland Security Advisory Council.** The Secretary of Homeland Security is establishing the Homeland Security Advisory Council (HSAC) effective April 1, 2003. **The Secretary has determined that the HSAC is necessary and in the public interest in connection with the performance of his**

duties. **The primary purpose of the HSAC will be to provide advice and recommendations to the Secretary on matters relating to homeland security. The HSAC will operate in an advisory capacity only.** This notice is being provided in accordance with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. The HSAC will terminate two years from the date of its establishment, unless extended by the Secretary.
Source: http://frwebgate5.access.gpo.gov/cgi−bin/waisgate.cgi?WAISdo cID=399619441532+0+0+0eve

[Return to top]

Emergency Services Sector

18. *April 03, New York Times* — **Circling protectively above New York City.** Once the war began, the federal government resumed patrolling the city's skies, though with a different approach. Rather than have fighter jets arcing overhead, the Department of Homeland Security has deployed several helicopters, including a couple of Black Hawks, and a couple of Cessna Citation II jets to patrol the Air Defense Identification Zone, which extends about 30 miles from each of the area's three major airports. **These helicopters and small jets do not carry any weapons. Instead, according to officials of the Federal Bureau of Immigration and Customs Enforcement, they provide an early−warning system for anything suspicious in the air.** The strategy essentially works this way: Sophisticated radar planes, normally used to monitor drug−smuggling traffic in the South and in the Caribbean, are now being used to detect suspicious aircraft long before they reach New York, as far north as the border with Canada.
Source: http://www.nytimes.com/2003/04/03/international/worldspecial /03BARR.html

[Return to top]

Information and Telecommunications Sector

19. *April 04, Electronic Times* — **DNS pioneer warns of Internet security. When it comes to the Domain Name System (DNS), the database architecture at the heart of the Internet infrastructure for the last 20 years, "the majority of the work to be done still lies ahead of us,"** said Paul V. Mockapetris who co−invented DNS in 1983. Mockapetris received the 2003 IEEE Internet Award for his pioneering work on DNS on Tuesday. Mockapetris warned that efforts need to be made to improve its security especially since the October 2002 attacks on 9 of the Internet's 13 DNS root−name servers that contain the master domain list for DNS and the March 27th 2003 hacker attacks on the al−Jazeera network, part of which were DNS−based. **Despite attacks that portend graver security breaches, Mockapetris noted that The Internet Engineering Task Force has not yet hammered out a standard** after nearly a decade of work. With a security model for DNS in place, extensions could be built onto DNS that would relate to creating greater opportunities on the Internet including phone numbers for IP telephony, distribution of security keys and certificates, and no−call lists for telemarketers. But without it, **there is a "real opportunity for fraud" as the hacker community climbs the technology ladder and puts the 30 million people with web domains at risk**, according to Mockapetris.
Source: http://www.electronicstimes.com/tech/news/OEG20030401S0048

20. *April 03, Associated Press* — **Six million mass text messages avert SARS panic. When a false Internet story about Asia's mystery illness sent fears through Hong Hong, authorities used a fast and simple way to shoot down the rumor: they sent a blanket text message to about 6 million mobile phones that denied the territory had been declared an "infected city."** Severe Acute Respiratory Syndrome, or SARS, has killed at least 78 people and sickened more than 2,200 worldwide. The government used the text message on Tuesday after the "infected city" hoax report appeared online, prompting panic among some residents who thought the territory would be shut down. The government's text response said: "Director of Health announced at 3pm today there is no plan to declare Hong Kong as an infected area." The hoax story was allegedly posted by a 14–year–old boy who was quoted as saying he did it for fun, and didn't think anybody would believe the story. **A telecommunications professor said mass text messaging – or SMS messaging – was justified in emergencies, but could potentially be abused**. "It's very important for phone operators to identify where the information comes from," said KL Ho, who teaches at the Department of Electrical and Electronic Engineering at the University of Hong Kong. "It's also very important to remind users not to believe just one single source," Ho said.
Source: http://www.news.com.au/common/story_page/0,4057,6232520%5E17 02,00.html

21. *April 02, Federal Computer Week* — **NIST security division expands role. The National Institute of Standards and Technology's (NIST) Computer Security Division will be playing a significant role in the Bush administration's cybersecurity strategy**, according to Howard Schmidt, acting chairman of the President's Cybersecurity Board. The NIST division did not move to the new Information Analysis and Infrastructure Protection (IAIP) Directorate at the Department of Homeland Security (DHS), as originally set out in the White House's plan. **Discussions are under way to determine how the organization can and will contribute to the implementation of the National Strategy to Secure Cyberspace**, Schmidt said. Schmidt also is working with the recently appointed IAIP directorate leaders to make sure that all of the work being done by the President's Critical Infrastructure Protection Board –– dissolved in a February executive order –– is carried over into DHS.
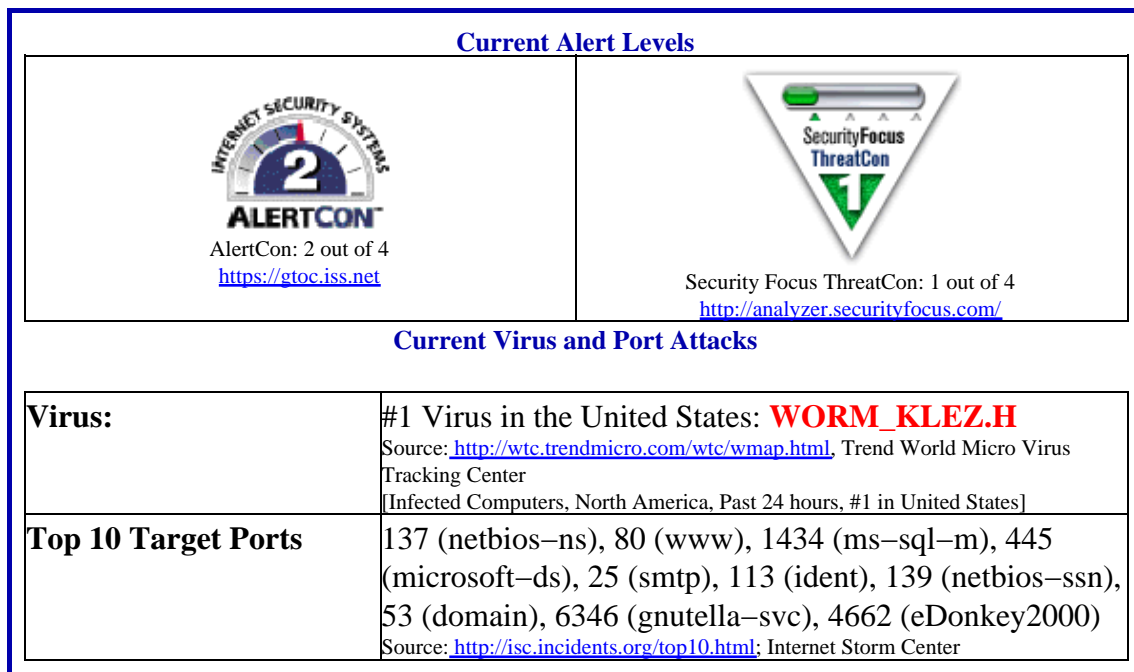Source: http://www.fcw.com/fcw/articles/2003/0331/web–schmidt–04–02– 03.asp

22. *April 02, CNET News.com* — **Holes found in RealPlayer, QuickTime. There are serious security holes in two popular digital media players: RealNetworks' RealPlayer and Apple Computer's QuickTime. In both cases, updates are available to remedy the problem**. RealNetworks is warning that by creating a specifically corrupted Portable Network Graphics file, an attacker could cause "heap corruption." Doing so would allow the attacker to execute code on the victim's machine. The vulnerable software uses an older data–compression library within the RealPix component of the player, leaving the system vulnerable. **The vulnerability affected the following versions of the software: RealOne Player, RealOne Player v2 for Windows, RealPlayer 8 for Windows, RealPlayer 8 for Mac OS 9, RealOne Player for Mac OS X, RealOne Enterprise Desktop Manager and RealOne Enterprise Desktop**. Meanwhile, security firm iDefense warned this week of **an exploitable buffer overflow vulnerability in versions 5.x and 6.0 of Apple's QuickTime Player that could affect computers with Microsoft's Windows**. A URL containing 400 characters will overrun the allocated space on the system, allowing the attacker to assume control of the system, iDefense said.

23. *April 01, National Journal* — **DHS may oversee Internet infrastructure.** The Bush administration's acting cybersecurity adviser Howard Schmidt said Tuesday that **homeland security and government agencies officials are working to formalize a security apparatus for the global Internet root servers, a series of computer systems that underpin the Internet's address system**. After an attack on those servers and the Internet domain−name system last October, Schmidt, several agencies officials, computer−security experts and root−server operators discussed in January how they could better respond to such incidents. **Their talks identified the need to develop a framework for determining when individuals and companies that operate the Internet's mission−critical domain system should report an attack or disturbance to government officials**.
Source: http://www.govexec.com/dailyfed/0403/040103td1.htm

Internet Alert Dashboard

Current Alert Levels	
AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: **WORM_KLEZ.H** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 80 (www), 1434 (ms−sql−m), 445 (microsoft−ds), 25 (smtp), 113 (ident), 139 (netbios−ssn), 53 (domain), 6346 (gnutella−svc), 4662 (eDonkey2000) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

24. *April 03, Reuters* — **Thailand tightens security after attack warning.** Thailand said on Thursday it had tightened security in tourist areas ahead of its biggest festival of the year after warnings of a possible attack by Muslim radicals on Westerners somewhere in Southeast Asia. **National Police Chief Sant Sarutanonda said police had received a tip−off from a Western country that a major attack might be planned as U.S. and British forces tightened their grip on Iraq. He declined to say which country had given the warning.** "There has been a warning from a western country to governments in Southeast Asia to beef up their security because they are worried that as the war intensifies, their citizens in Asia will be attacked," Sant

told reporters. Thailand celebrates its traditional New Year Songkran water festival from April 12 to 15, an event that usually attracts tens of thousands of tourists.
Source: http://www.washingtonpost.com/wp−dyn/articles/A18706−2003Apr 3.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129
Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.	

Contact DHS/IAIP
To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer
The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.